

CLAIMS

What is claimed is:

- 1 1. A method for capturing illegal and undesired behavior for network components and
2 for interactions between components comprising:
3 specifying one or more states and state transitions for one or more components or
4 interactions between two or more components, wherein specifying includes specifying at
5 least one composite state transition; and
6 if a said state or state transition occurs, generating a notification corresponding to the
7 specified state or state transition.
- 1 2. The method recited in claim 1, wherein said states are specified based on thresholds.
- 1 3. The method recited in claim 1, wherein the notification is an event.
- 1 4. The method recited in claim 1, wherein a state or state transition is a state or state
2 transition of a component, and wherein the step of generating the notification comprises
3 generating the notification by the component.
1
- 1 5. The method recited in claim 1, wherein if the state or state transition relates to an
2 interaction between components, and wherein the notification is generated by at least one of
3 the components involved in the interaction between the components.
- 1 6. The method recited in claim 1, further comprising the step of:
2 reporting the notification to a network management system.

- 1 7. The method recited in claim 1, further comprising the step of:
2 detecting whether a state or state transition has occurred; and
3 wherein if said step of detecting detects that a state or state transition has occurred,
4 said notification is generated in response to said step of detecting.
- 1 8. The method recited in claim 7, wherein, the step of detecting is performed by an
2 agent.
- 1 9. The method recited in claim 8, wherein the agent is a dedicated agent.
- 1 10. The method recited in claim 1, further comprising the step of polling said components
2 to determine whether a state or state transition has occurred.
- 1 11. The method recited in claim 1, wherein the step of specifying one or more states and
2 state transitions comprises specifying illegal states.
- 1 12. The method recited in claim 1, wherein the step of specifying one or more states and
2 state transitions comprises specifying undesired states.
- 1 13. The method recited in claim 1, wherein the step of specifying one or more states and
2 state transitions comprises specifying illegal states and undesired states.

1 14. The method recited in claim 6, wherein detecting whether a state or state transition
2 has occurred comprises determining whether a component or component interaction has
3 entered an illegal or undesired state.

1 15. The method recited in claim 11 wherein an authorization violation and an
2 authentication forgery are defined as illegal states.

1 16. The method recited in claim 12, wherein a nongracefully QoS degradation is defined
2 as an undesired state.

1 17. The method recited in claim 1, further comprising the step of examining multiple
2 notifications to deduce trends regarding the network.

1

1 18. The method recited in claim 17, wherein the step of examining multiple notifications
2 comprises examining notifications for stable-behavior in a threshold value.

1 19. The method recited in claim 17, wherein the step of examining multiple notifications
2 comprises examining notifications for increases or decreases in a threshold value.

1 20. A system for capturing illegal and undesired behavior for network components and
2 for interactions between components, the system comprising:
3 one or more network components configured to spontaneously generate notifications
4 upon the occurrence of specified states and state transitions, including one or more
5 composite state transitions; and

6 a network management system configured to receive said spontaneously generated
7 notifications.

1 21. The system of claim 20, further comprising:
2 an agent configured to detect the generation of notifications by the network
3 components, and configured to report detected notifications to said network management
4 system.

1 22. The system of claim 20, further comprising:
2 a state table configured to store said specified states and state transitions, including
3 composite state transitions.

1 23. The system of claim 21, wherein the state table is in a network management system.

1 24. The system of claim 21, wherein the state table is in a network component.

1 25. The system of claim 22, wherein the agent is further configured to examine one or
2 more conditions of one or more network components and to query the state table to
3 determine whether the one or more conditions represents an illegal or undesired state.

1 26. The system of claim 22, wherein the agent is further configured to examine one or
2 more transitions relating to one or more network components and to query the state table to
3 determine whether the one or more transitions represents an illegal or undesired transition.

1 27. A system for capturing illegal and undesired behavior for network components and
2 for interactions between components comprising:
3 one or more network components;
4 an agent configured to examine said network components to determine whether
5 specified states or state transitions, including composite state transitions, have occurred,
6 wherein the agent is configured to generate notifications upon a determination that a
7 specified state or state transition has occurred, and wherein the agent is configured to report
8 detected notifications to said network management system; and
9 a network management system configured to receive reports of said generated
10 notifications.

1 28. The system of claim 27, further comprising:
2 a state log configured to store said specified states and state transitions, including
3 composite state transitions.

1 29. A computer-readable medium carrying one or more sequences of instructions for
2 capturing illegal and undesired behavior for network components and for interactions
3 between components, which instructions, when executed by one or more processors, cause
4 the one or more processors to carry out the steps of:
5 specifying one or more states and state transitions for one or more components or
6 interactions between two or more components, wherein specifying includes specifying at
7 least one composite state transition; and
8 if a said state or state transition occurs, generating a notification corresponding to the
9 specified state or state transition.

1 30. A computer-readable medium as recited in Claim 29, wherein said states are specified
2 based on thresholds.

1 31. A computer-readable medium as recited in Claim 29, wherein said notifications are
2 events.

1 32. A computer-readable medium as recited in Claim 29, wherein a state or state
2 transition is a state or state transition of a component, and wherein the step of generating a
3 notification comprises generating the notification by the component.

1

1 33. A computer-readable medium as recited in Claim 29, wherein if the state or state
2 transition relates to an interaction between components, and wherein the notification is
3 generated by at least one of the components involved in the interaction between the
4 components.

1 34. A computer-readable medium as recited in Claim 29, wherein the instructions for
2 carrying out the step of creating and storing first information further comprise instructions
3 for carrying out the step of:
4 reporting the notification to a network management system.

1 35. A computer-readable medium as recited in Claim 29, wherein the instructions for
2 carrying out the step of creating and storing first information further comprise instructions
3 for carrying out the steps of:
4 detecting whether a state or state transition has occurred; and

5 wherein if said step of detecting detects that a state or state transition has occurred,
6 said notification is generated in response to said step of detecting.

1 36. A computer-readable medium as recited in Claim 35, wherein the step of detecting is
2 performed by an agent.

1 37. A computer-readable medium as recited in Claim 36, wherein the agent is a dedicated
2 agent.

1 38. A computer-readable medium as recited in Claim 29, wherein the instructions for
2 carrying out the step of creating and storing first information further comprise instructions
3 for carrying out the step of:
4 polling said components to determine whether a state or state transition has occurred.

1 39. A computer-readable medium as recited in Claim 29, wherein the step of specifying
2 one or more states and state transitions comprises specifying illegal states.

1 40. A computer-readable medium as recited in Claim 29, wherein the step of specifying
2 one or more states and state transitions comprises specifying undesired states.

1 41. A computer-readable medium as recited in Claim 29, wherein the step of specifying
2 one or more states and state transitions comprises specifying illegal states and undesired
3 states.

1 42. A computer-readable medium as recited in Claim 35, wherein detecting whether a
2 state or state transition has occurred comprises determining whether a component or
3 component interaction has entered an illegal or undesired state.

1 43. A computer-readable medium as recited in Claim 39, wherein an authorization
2 violation and an authentication forgery are defined as illegal states.

1 44. A computer-readable medium as recited in Claim 40, wherein a nongracefully QoS
2 degradation is defined as an undesired state.

1 45. A computer-readable medium as recited in Claim 29, wherein the instructions for
2 carrying out the step of creating and storing first information further comprise instructions
3 for carrying out the step of examining multiple notifications to deduce trends regarding the
4 network.

1

1 46. A computer-readable medium as recited in Claim 45, wherein the step of examining
2 multiple notifications comprises examining notifications for stable-behavior in a threshold
3 value.

1 47. A computer-readable medium as recited in Claim 45, wherein the step of examining
2 multiple notifications comprises examining notifications for increases or decreases in a
3 threshold value.